HP セキュリティ・ソリューション

ネットワーク化された世界、それはリスクとも繋がっています

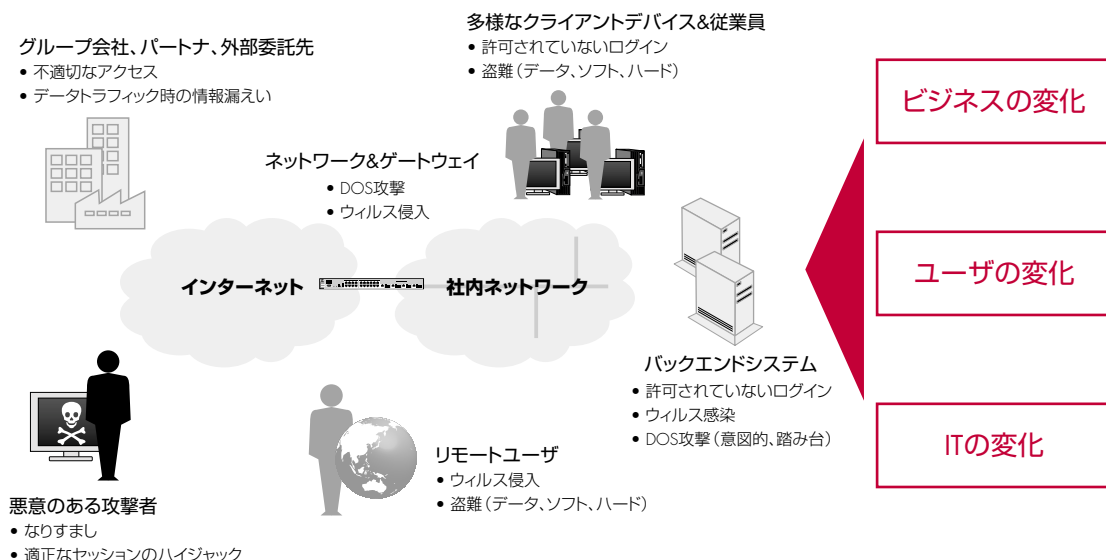
ビジネス推進の原動力となったIT。今のままのセキュリティ対策でビジネスの成功に不安はありませんか？

ITの成果がビジネスに直結するようになった今、
ITの価値は、もはやビジネスをどれだけ支えるかではなく、
ビジネスの成果にどれだけ貢献できるか、へとシフトしています。
「ビジネスの成長と加速」を可能にする俊敏性の高い安全なIT環境を
低コストで実現するうえで、ITセキュリティの果たすべき役割は重大です。

しかし、変化し続けるビジネス環境、IT環境の複雑化、テクノロジの進化は
最適なITセキュリティの実現を困難なものにしています。
こうした状況に対応するには、
セキュリティツールや個別システム毎の対策から、IT環境全体にわたり、
常に一貫性と整合性を備えたセキュリティ対策を遂行できる
「ITセキュリティ・インフラストラクチャ」の構築という視点が重要です。

HPは、企業のITセキュリティ・インフラストラクチャ構築を支援する
総合的なソリューションを提供します。

ビジネスへのリスク波及を総合力で確実に防止する HP セキュリティ・ソリューション

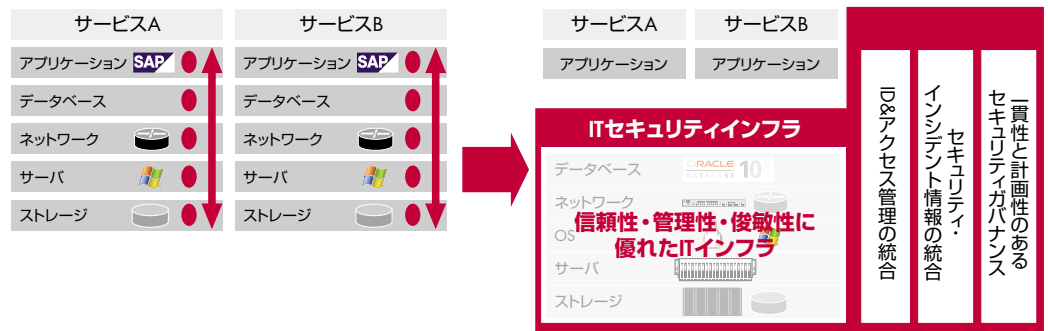
多様化するリスクの要因

セキュリティ対策の不備による損害は部署や企業の壁を超えて、果てしなく広がる

今日のITはネットワーク化され、企業内の部署や部門、さらには企業の枠を超えて連携が可能になっています。オフィス内には正社員や契約社員をはじめとする多様な人々がともに働き、モバイル機器を使ったオフィス外からのリモートアクセスも当たり前になっています。業務提携やアウトソーシング、Webを介したビジネス連携などが進展したことで、社外の人々ともネットワークでつながっています。その一方で、悪意ある外部からの攻撃はますます高度化・悪質化しています。また、内部者からの情報漏えいにも目を光らせなくてはなりません。複雑化したビジネス環境とITシステム、さらに進化を続けるITテクノロジ、高い専門性が要求されるセキュリティ人材の不足の中で、ビジネスを阻害することなく情報資産の安全性と可用性を維持・保証するには、あまりにも多くの課題が存在しています。

ビジネス成長に貢献できる俊敏性の高いIT環境を実現するためにITセキュリティ・インフラストラクチャを整備する時代

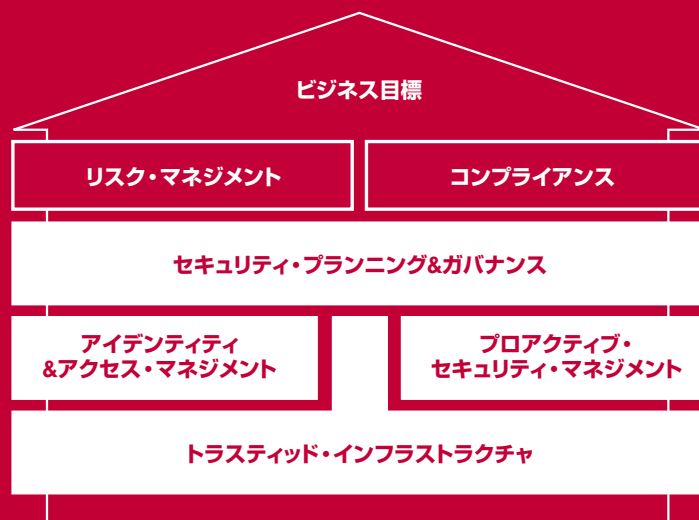
従来のセキュリティ対策で行なってきたシステムごと、ツールごとの個別の対策に限界を迎えた今、セキュリティのアプローチは次のステージへ進むべき時がきています。
安全なIT環境をビジネスニーズに応じて俊敏に提供するには、ITの今後の利用形態も考慮した全社的・長期的な視点で、セキュリティの運用プロセス・テクノロジ・ポリシの標準化を推進し、強いガバナンス力を全てのIT環境に遂行することが重要です。その結果、「コスト」「品質」「納期」のバランスがとれた合理的なセキュリティ対応が可能になるのです。このような一貫性のある総合的なITセキュリティ対策を実現するために、これからは、企業内の全てのIT利用に対して提供されるサービスとしてITセキュリティをとらえた、「ITセキュリティ・インフラストラクチャ」を整備するという発想が重要です。

IT環境全体にセキュリティを組み込み
効果と効率を最大化させる
HPの「ITセキュリティ・インフラストラクチャ」という思想

ITセキュリティ・インフラストラクチャへの変革

ITセキュリティ・インフラストラクチャの特長

従来のITセキュリティ対策	これからのITセキュリティ対策
必要に応じた個別対応 必要に応じて個別のセキュリティ対策を導入してきた結果、全体感のない対応策となり、管理負荷やリスクの増大。	**計画性、一貫性のある対策** ITセキュリティ対策をシンプル化・標準化してサービスとしてバリューチェーン全体に提供。全てのITシステムのライフサイクルを通じて、一貫したセキュリティポリシを実装する。
部分的なセキュリティマネジメント 個別のセキュリティツールを導入してきた結果、全体の運用管理の負荷が増大。問題発生の特定・対応などが困難でリスクが増大。	**連携・統合されたセキュリティマネジメント** セキュリティ運用の各プロセスを標準化して、連携・統合化。管理対象全てを網羅して、全体としてのリスクを可視化できるだけでなく、管理負荷を改善しながら、ひとつひとつの対策効果を向上させる、統合的なリスク管理を実行。
ばらばらなユーザ管理 アプリケーション毎に独自のパスワード管理、ユーザ管理、アクセス制御を行なっているため、利用者、システム管理者ともにセキュリティ上の手間が増加。	**統合されたID・アクセス管理** 多様なアプリケーションに共用できるID・アクセス管理の統合管理基盤で、ユーザへの迅速なアクセス提供と統制を両立。
「アドオン」型セキュリティ システム、ネットワークへセキュリティツールをアドオンする対応を中心としたため、セキュリティメカニズムが複雑化し、全体のセキュリティレベルにもばらつきが発生。	**「ビルトイン」されたセキュリティ** ハードウェアやOS、ネットワークに実装されたセキュリティでセキュリティの実装をシンプル化。組み合わせによる、強固なセキュリティの基礎を構築。
特定技術への依存 独自の技術や製品に依存するセキュリティ対策を行ってきた結果、相互運用性が低下。新技術の採用が遅れ、システム全体の俊敏性が低下。	**オープン・スタンダードの採用** 業界標準ツール、プロトコル、ハードウェア、OSを採用し、相互運用性・柔軟性に優れたセキュリティ対策を実行。

ITセキュリティ・インフラストラクチャの構築と運用を支援するHPのセキュリティ・ソリューションファミリー

ビジネスの成長を加速する安全で柔軟なIT環境の実現にむけて
ITセキュリティ・インフラストラクチャの効率的な構築と改善を支援する
HPの包括的なセキュリティ・ソリューション・ファミリーをご紹介します。

セキュリティ・プランニング&ガバナンス

••• P4

情報セキュリティ対策は リスクアセスメントと情報セキュリティ・ポリシー策定から

考慮すべき範囲が広いセキュリティ対策では、まず最初のセキュリティ・ポリシーとこれに基づいた実施のための環境作りをしっかりと固める必要があります。場当たり的に対策を進めてしまうと後々に大きな影響が及んでしまいます。

- セキュリティ・アセスメント
- セキュリティ・ポリシー体系策定支援
- セキュリティ・アドバイザリー
- アイデンティティ&アクセス・マネジメント アーキテクチャ・コンサルティング

アイデンティティ&アクセス・マネジメント

••• P6

万全なユーザ認証と認可、そしてIDのライフサイクル管理と監査対応に要する運用効率向上と迅速な情報アクセスの提供

企業内の多様な勤務形態、コンプライアンス強化のための職務分掌の明確化などに対応するには、的確で一貫したアイデンティティ管理とアクセス制御が不可欠です。

- シングル・サインオン・ソリューション
- 統合ID管理ソリューション
- 認証連携ソリューション
- モニタリング・監査対応ソリューション

プロアクティブ・セキュリティ・マネジメント

••• P8

複雑なセキュリティ対策の統合的な運用で、セキュリティリスクの抑制と運用コスト削減に貢献

企業のITシステム全体に渡るセキュリティリスクの把握から対策、そして予防、報告まで効果的かつ効率的に実現するための、プロアクティブなセキュリティマネジメント環境を提供します。

- イベント・インシデント管理ソリューション
- 統合ログ管理ソリューション
- 脆弱性管理ソリューション
- 変更・構成管理ソリューション

トラステッド・インフラストラクチャ

••• P10

セキュリティ機能をビルトインしたプラットフォーム、OS、ネットワークでシステム設計のシンプル化と可用性を確保

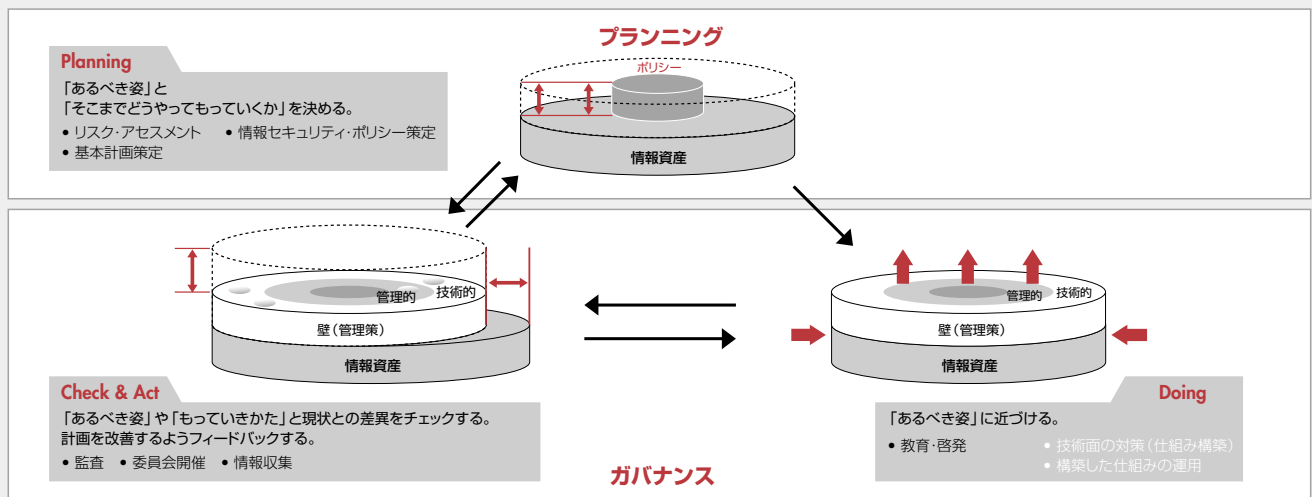
ITインフラを構成する多様な機器やソフトウェアに、あらかじめセキュリティ機能がビルトインされていれば、セキュリティ環境整備に要する負担は大きく軽減されます。トラステッド・インフラストラクチャでは、相互運用性にも優れたビルトイン型セキュリティに対応した広範な製品とソリューションを提供します。

- HP製品群のビルトイン・セキュリティ機能
- ネットワーク仮想閉域網ソリューション
- ネットワーク・アクセス制御ポリシー・統合管理ソリューション
- クライアント認証・検疫ソリューション
- HP クライアントPC統合（CCI）ソリューション

セキュリティ・プランニング&ガバナンス

情報セキュリティ対策は
リスクアセスメントと情報セキュリティ・ポリシー策定から

日本HPは、HPワールドワイドでの長年にわたる情報セキュリティへの取り組みと、
日本における豊富な情報セキュリティ・ポリシー策定支援の経験を生かし、
セキュリティのプランニングとガバナンスをお手伝いします。

セキュリティ・プランニング&ガバナンスのPDCAサイクル

〈HPが提供する主なソリューション〉

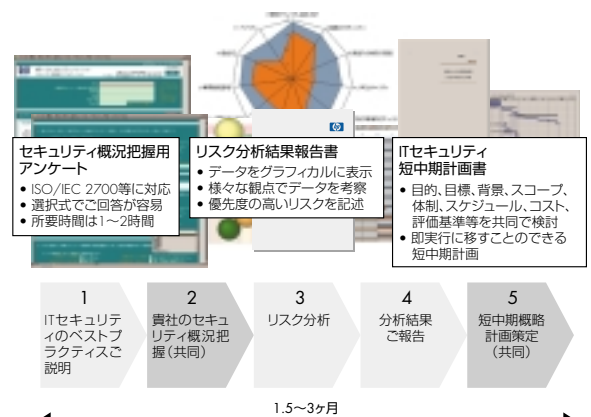
セキュリティ・アセスメント

セキュリティ対策として実施すべきことは、技術面から管理面まで多岐にわたります。計画がないまま進めてしまうと、せっかくの対策も無駄な投資に終わってしまう可能性が高くなります。堅実なのは詳細リスク分析から始めることです。しかし、これに時間がかかるとその間にリスクが現実化してしまう恐れがあります。最初のリスクアセスメントはできるだけ短期間で行なう必要があるのです。

●対象となるお客様

- 情報セキュリティ上の弱点を知りたい
- 情報セキュリティ対策計画を策定したい

●ソリューションの特長

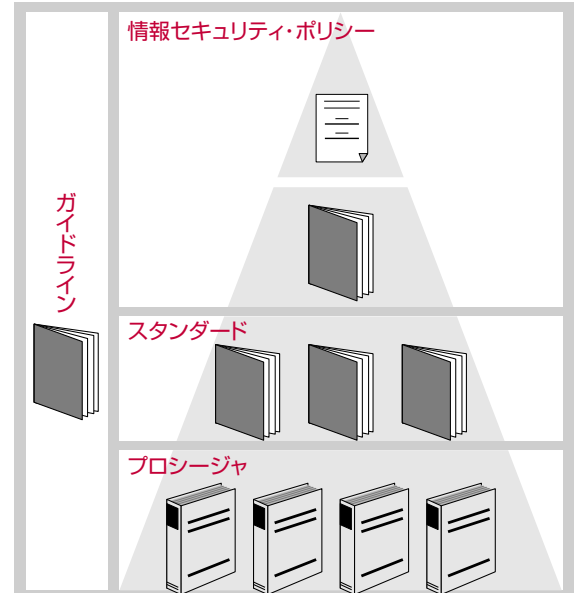
- ISO/IEC27001をベースにリスクアセスメントを短期間で実施
- リスクアセスメントに基づく情報セキュリティ対策の短中期計画を策定

セキュリティ・ポリシー体系策定支援

情報セキュリティ・ポリシーの必要性は常識化していますが、厳しすぎる規則によるモチベーションや業務効率の低下、利用者に理解されない不適切な表現、法律順守に必要な事項の欠落など、有効な情報セキュリティ・ポリシーの策定は容易ではありません。また、一度策定すれば済むものではなく、ビジネス環境やIT環境の変化の中でセキュリティを継続するには、既存の情報セキュリティ・ポリシーを見直すことも必要になっています。

●対象となるお客様

- 情報セキュリティ・ポリシーを策定・見直したい
- 情報セキュリティ・ポリシーを機能させるためのスタンダードやプロシージャ、ガイドライン等を策定したい

●ソリューションの特長

- ビジネスプロセスや組織形態に応じた情報セキュリティ・ポリシーの策定・改善支援
- 情報セキュリティ・ポリシーを機能させるためのスタンダードやプロシージャ、ガイドライン等の策定支援

セキュリティ・アドバイザリー

情報セキュリティ・ポリシーや対策計画を策定したとしても、それだけで実際のリスクが減るものではありません。これらを現実に機能させるためには、情報セキュリティ委員会の設立から運営、関係者の啓発や教育、具体的対策への落としこみ等、様々な取り組みが必要になります。

さまざまなシーンでのコンサルティング

情報セキュリティ委員会の設立

啓発・教育

文書整備

●対象となるお客様

- 「セキュリティ・ポリシー体系策定支援」により情報セキュリティ・ポリシーを策定され、それに準じて対策を実施しようとされているお客様
- 「セキュリティ・アセスメント」により長・短期計画を策定され、それに準じて対策を実施しようとされているお客様
- セキュリティ対策実施に関するメニュー外のコンサルテーションをお望みのお客様

●ソリューションの特長

- 本サービスでは、情報セキュリティ・ポリシーや対策計画を現実に機能させるためのコンサルティングによる支援を提供します。
  (通常、他のセキュリティ・プランニング&ガバナンス・サービスからの継続サービスとして提供します。)

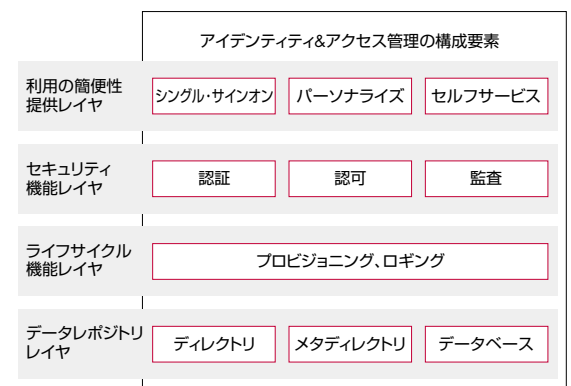
アイデンティティ&アクセス・マネジメント　アーキテクチャ・コンサルティング

アイデンティティ&アクセス・マネジメントの実現にはディレクトリ、シングル・サインオン、認証、IDプロビジョニングなど、多くの技術を最適に組み合わせ基盤として構築する必要があります。局所的な個別最適化ではなく、多くの利用者やシステムに柔軟に対応できる、今後の利用状況・技術動向を踏まえた統合的なアーキテクチャを策定する必要性が高まっています。

●対象となるお客様

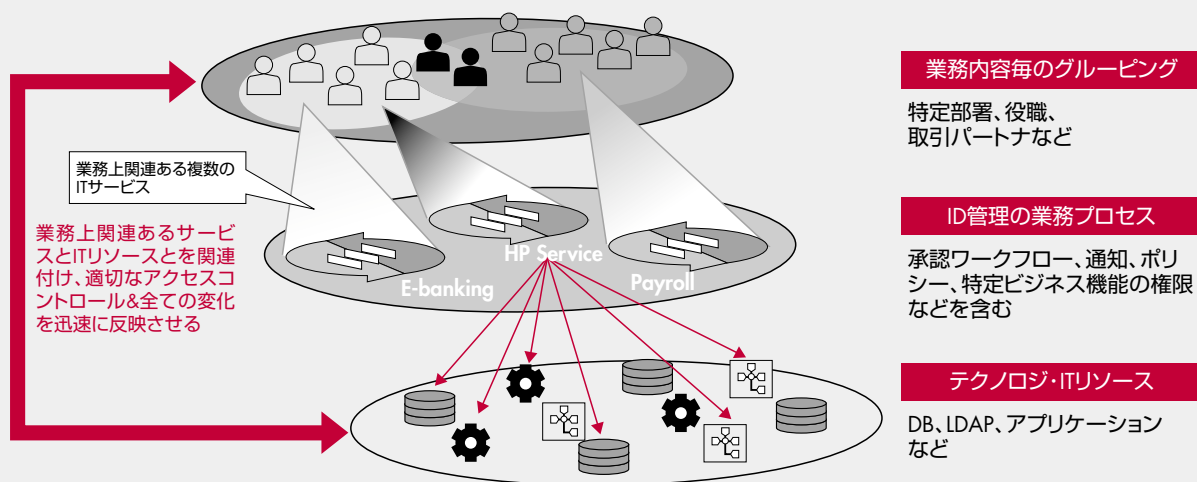
- 今後、IDやアクセス管理のための全社的な基盤を検討・構築したい
- 既存のID管理・アクセス管理の課題をまとめ、対応策を考えたい

●ソリューションの特長

- HPでの実績に基づく、アイデンティティ&アクセス・マネジメント・フレームワークの利用と国内での実績
- 現状分析・課題抽出に基づき、最適なアーキテクチャをデザインし、実現のロードマップを策定。

アイデンティティ&アクセス・マネジメント

万全なユーザ認証と認可、
そしてIDのライフサイクル管理、監査対応に要する
運用効率向上と迅速な情報アクセスの提供

HPのアイデンティティ&アクセス・マネジメントは、変化するIDのライフサイクル管理において、
アイデンティティ&アクセス・マネジメント（I&AM）の業務プロセスからポリシー、ITリソースまでを紐付けた
「I&AMのサービス」という単位で管理が可能なテクノロジアーキテクチャにより、
さまざまな要素が関連するID管理の自動化を可能にします。

これからのアイデンティティ&アクセス・マネジメント

〈HPが提供する主なソリューション〉

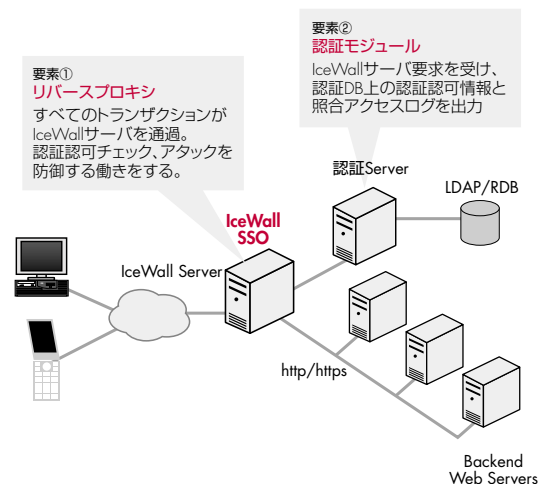
シングル・サインオン・ソリューション

国内トップシェアを誇るHP IceWall SSOが、各Webアプリケーションへのシングル・サインオン・認可・監査証跡取得を代行し、Webサービスへの一元的なアクセス管理を行ないます。これにより、堅牢な認証基盤の構築が可能になります。

●対象となるお客様

- 各Webアプリケーションへのログインを一元化したい
- 認証、認可を統合し、Webアクセスログを一元管理したい
- 管理コストを抑制しながら、堅牢な認証基盤を構築したい

●ソリューションの特長

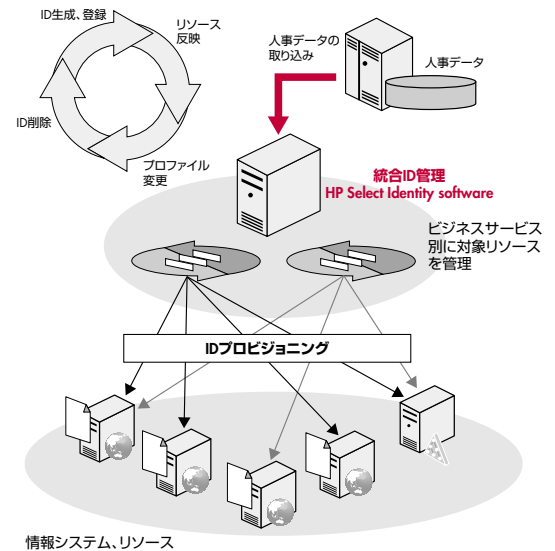
- 国内No.1の実績を持つWebSSOソリューション、HP IceWall
- プラットフォームを選ばないエージェントレスのリバースプロキシ方式を採用
- 数百万規模にも対応できるパフォーマンス、スケーラビリティ
- 充実したAPIによる他の認証機能との組み合わせで、ユーザ認証のさらなる強化が可能
- Webアクセスログの統合的な取得が可能

統合ID管理ソリューション

システムやサーバ、リソースに分散した多くのID情報を関連付け、ユーザIDのライフサイクル管理を効率的に行なえるサービス指向型の統合ID管理環境の構築をサポート。幽霊アカウントや職務分掌の曖昧さをなくし、内部統制の要請する適正なID管理を実現できます。

●対象となるお客様

- IT統制を強化するため、分散したIDを一元管理したい
- 共有IDから個人IDへ移行して、職務分掌の確実性を確保したい
- ID情報の変更・削除などの対応を迅速かつ確実に行ないたい

●ソリューションの特長

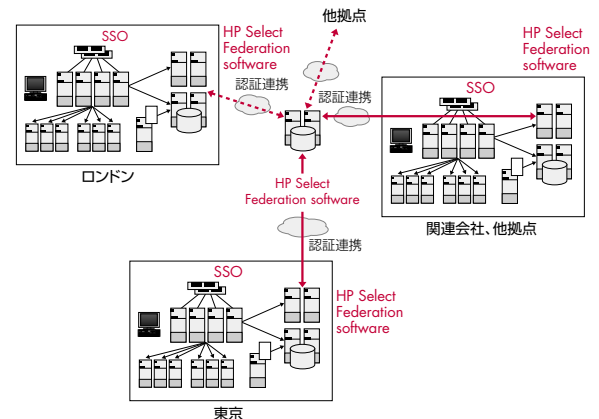
- IDプロビジョニングによりID情報をITシステムやリソースに迅速に反映
- 大規模環境でも正確なID管理を効率的に実現
- 監査対象となる全てのプロビジョニングログを記録し、他のモニタリング・監査レポーティングソリューションとの連携が可能
- ユーザ自身でパスワード変更可能なセルフサービス機能
- 主なOS、アプリケーション、データベースへの標準対応

認証連携ソリューション

グループ企業・海外拠点との連携や他企業との協業、複数のBtoCサイトをつないだサービス提供モデルでスムーズな認証連携が実現できれば、ビジネスの加速に大きく貢献します。HPの認証連携ソリューションは、サイトごとに異なる認証システム間で利用可能な認証連携(グローバル・シングル・サインオン)を実現します。

●対象となるお客様

- 各企業で管理された信頼あるIDを利用して企業間連携したい
- 自社管理IDを利用したBtoCサイトのサービス連携で提供サービスの拡充を図りたい

●ソリューションの特長

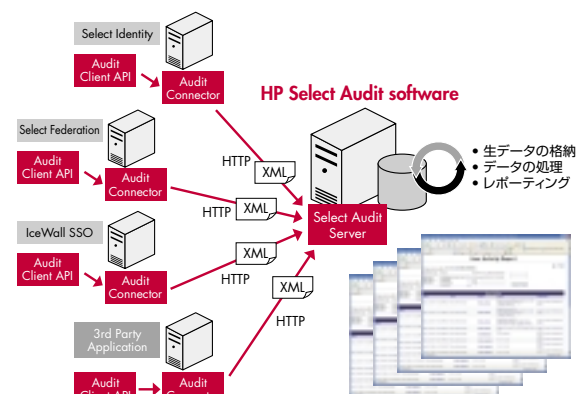
- HP IceWall SSOはもちろん多様なSSO製品との認証連携が可能
- Liberty、SAML、WS-Federationなどの最新規格に対応
- 認証連携の容易な設定を可能にするWebGUIを採用
- 強力なユーザのプライバシー保護機能を実現

ID管理　監査対応ソリューション

内部統制や法制度(金融商品取引法など)への対応には、ID・アクセス管理状況の「見える化」が必要です。多岐にわたるユーザやITリソースにより、内部・外部監査時には、この「見える化」の作業負荷が懸念されます。HPのID管理　監査対応ソリューションは、監査に必要な情報の収集・安全な保管や相関分析、レポート作成を自動化し、対応の効率化とコンプライアンス強化に貢献します。

●対象となるお客様

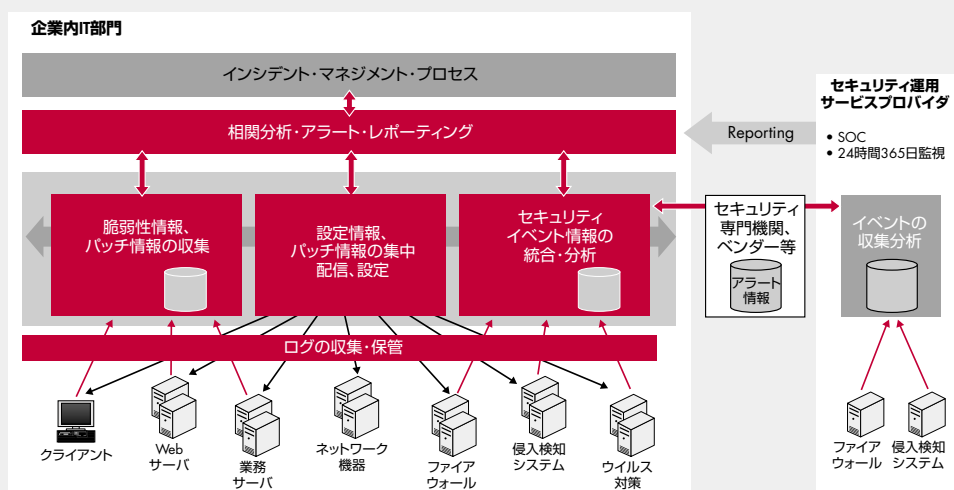
- 監査で必要となる、アクセス制御等に関する監査証跡をとりたい
- ITリソースへの正規ユーザのアクセス状況を知りたい
- ID作成・変更・削除のプロセスを記録して、問題箇所を特定したい

●ソリューションの特長

- SOXレポートパックにより、監査レポートのテンプレートを提供
- HPのID管理ツールの他、他社管理ツールとも連携し、情報収集の一元化が可能

プロアクティブ・セキュリティ・マネジメント

複雑なセキュリティ・インシデント管理の統合的な運用で、セキュリティリスクの抑制と運用コスト削減に貢献

HPのプロアクティブ・セキュリティ・マネジメントは、多様なセキュリティ脅威管理や脆弱性管理、インシデント管理の統合化を目指したソリューション群です。
ITシステム全体でのセキュリティ脅威の把握から対策・分析・予防・評価・報告までの管理プロセスを構築し、従来の事後対応を主としたリアクティブな環境を、プロアクティブなセキュリティ・マネジメントへと変革します。

全社レベルでのリスク把握と対策実施

〈HPが提供する主なソリューション〉

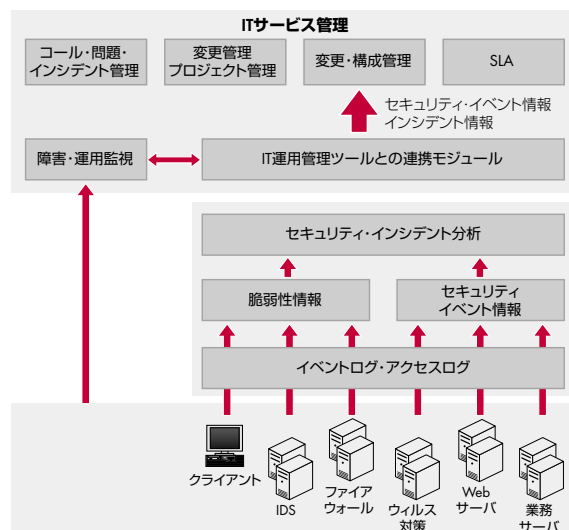
イベント・インシデント管理ソリューション

様々なセキュリティツールから出されるセキュリティイベントを収集、分析して重大なインシデントを特定し、リスク分析の観点から対応策の優先順位付けを行ないます。また、統合管理システムと連携することで、運用オペレータは、ネットワーク、サーバ、アプリケーションの監視と同じようにセキュリティ監視を効率的に行なうことができるため、セキュリティ・インシデント対応の迅速性も向上します。

●対象となるお客様

- 様々なセキュリティデバイスから大量のアラート情報が発行されるため、解析に手間がかかる
- 個々の対応のために本当の脅威が発見できず、対応が遅れる

●ソリューションの特長

- ITILベースのITサービス管理とセキュリティ・インシデント管理を連携・統一化するプロセス設計
- HPソフトウェア製品群の連携によるエンド・ツー・エンドの効率化を実現

統合ログ管理ソリューション

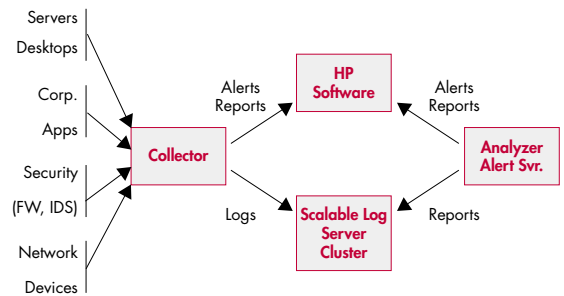
インシデント発生後の迅速なトラッキングや発生前の早期発見、不正の抑止には、システムログの活用が有効です。このシステムログを有効活用するため、HPの統合ログ管理ソリューションは、様々なログの相関分析をふまえた、大量かつ多様なログ内容の統一化やログ蓄積のシステムを提供します。

●対象となるお客様

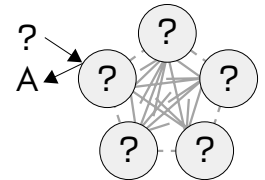
- 内部統制で要請されるシステムログの記録・保存を行ないたい
- 各システムで異なるログの収集レベルを標準化したい
- インシデント管理やセキュリティ分析のためにログを有効活用したい

●ソリューションの特長

- 超高速な大量ログ収集・検索・分析性能
- ログデータの超圧縮技術によるストレージコスト抑制が可能
- 高可用性アーキテクチャによるログ取得ミス、性能低下の回避
- 多様なログ・フォーマットへの対応に加え、アダプタの作成によりカスタムログも柔軟に取り込み可能

約180種類のログに対応済み

リアルタイム分析の他、長期間のログに関する相関分析が可能

Analyzer Cluster技術により、高速分散ログ分析を実現

60台のサーバ構成をとることで、速度が最大35000件/秒

脆弱性管理ソリューション

HPの脆弱性管理ソリューションは、ハイリスクな脆弱性を特定するために、ITインフラの脆弱性をスキャンして、脆弱性状況のデータを自動作成します。様々なOSやプラットフォームが混在する大規模環境で、定期的な脆弱性検査や問題特定の効率化、ポリシー遵守状況の把握を実現し、監査時の報告や改善対応のための警告に利用することができます。

●対象となるお客様

- セキュリティ監査を行いたいが、ノウハウがない
- サーバ設定状況のポリシ遵守状況を把握したい
- マルチプラットフォームや多数のサーバ、遠隔地のサーバ環境の調査を行いたい
- 脆弱性管理プロセスを標準化して、体系的に行ないたい

●ソリューションの特長

- 定期的な検査の自動化が可能
- 多様なOS・サーバへの標準対応、及び、リモート機能による遠隔地も含めた集中管理が可能なため全社標準ツールとして利用可能
- ポリシ作成作業を低減するテンプレートの提供

セキュリティポリシー
セキュリティ基準、実施手順

ポリシーに基づき、サーバの
監査項目を選択

監査ツールを使って監査

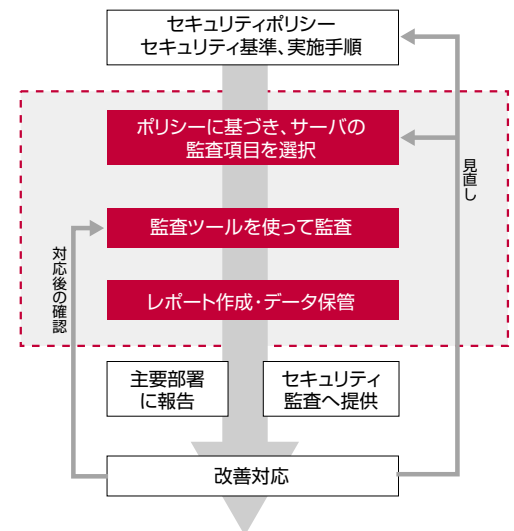
レポート作成・データ保管

対応後の確認

見直し

主要部署
に報告

セキュリティ
監査へ提供

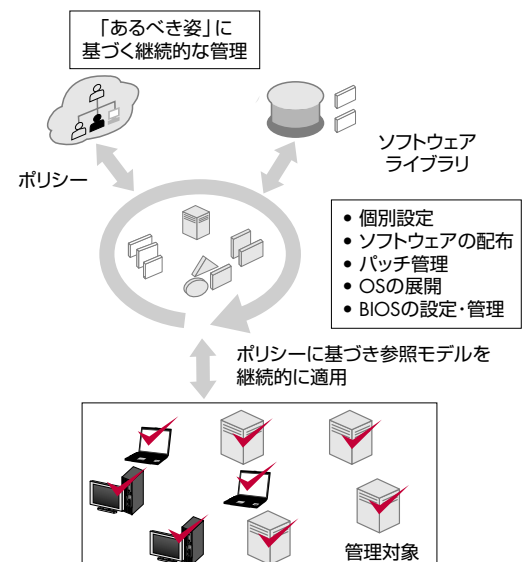
改善対応

変更・構成管理ソリューション

HPの変更・構成管理ソリューションは、非常に多くのクライアント端末、サーバ環境において、確実にセキュリティ要件を満たすため、セキュリティソフトウェアの更新やパッチ適用などの必要な対策を効率的に実施。ユーザ及び機器単位での構成情報のインベントリ収集・プロビジョニング・変更履歴監査など、管理対象のライフサイクルにわたる一元的な管理を可能にします。

●対象となるお客様

- ハードウェア、OS、アプリケーションなどの構成情報を把握したい
- アップデートやセキュリティパッチ適用を確実にしたい

●ソリューションの特長

- エージェントレスのディスカバリ機能とWBEMなど標準に基づくインベントリ収集機能
- BIOSなどハードウェア設定からOSの展開、パッチ管理、ソフトウェア配布など、クライアントやサーバのプロビジョニングを実行
- Windows、Linux、Unixなど混在環境をサポート

トラステッド・インフラストラクチャ

セキュリティ機能をビルトインした プラットフォーム、OS、ネットワークで システム設計のシンプル化と可用性を確保

広範なインフラテクノロジを提供するHPは、業界における標準化を推進し、
相互運用可能なビルトイン型セキュリティの開発に積極的に取り組んでいます。
こうした活動をベースに、データセンタからネットワーク、デスクトップまで、エンド・ツー・エンドの
「トラステッド・インフラストラクチャ」と、これらを組み合わせたソリューションを提供しています。

〈HP製品群のビルトイン・セキュリティ機能〉

オペレーション・システム層

■ HP-UX 11i v2/v3

HP-UX 11i v2は、セキュリティ評価基準であるISO15408(Common Criteria)のCAPP(ControlledAccess Protection Profile)およびRBAC-PP(Role-based ProtectionProfile)について認証取得済み※のOSです。軍事用セキュアOS機能として開発されたセキュリティ・コンパートメント機能(セキュリティ攻撃をサーバ内に封じ込める機能)を標準搭載し、HPの仮想化／ワークロード管理システムと組み合わせることで、セキュリティ攻撃によるダウンタイムを限りなくゼロに近づけることのできる、可用性の高いアプリケーションシステムが構築できます。さらに、アクセスコントロール機能として、OSに登録された役割ごとにルートユーザのアクセス権限を個別に設定できるロールベース・アクセス・コントロール(RBAC)機能を搭載しており、この管理をGUIベースで効率的に行えるHP software製品と組み合わせて、業務プロセスの職務分掌をOSレベルで反映し、アプリケーションへのアクセス管理環境を改善できます。また、ファイルをアプリケーションから透過的に自動で暗号化する機能(EVFS)を標準搭載しています。

※HP-UX11i v3については、認定作業中(2007年4月11日現在)

プラットフォーム層

■ HP Integrityサーバ

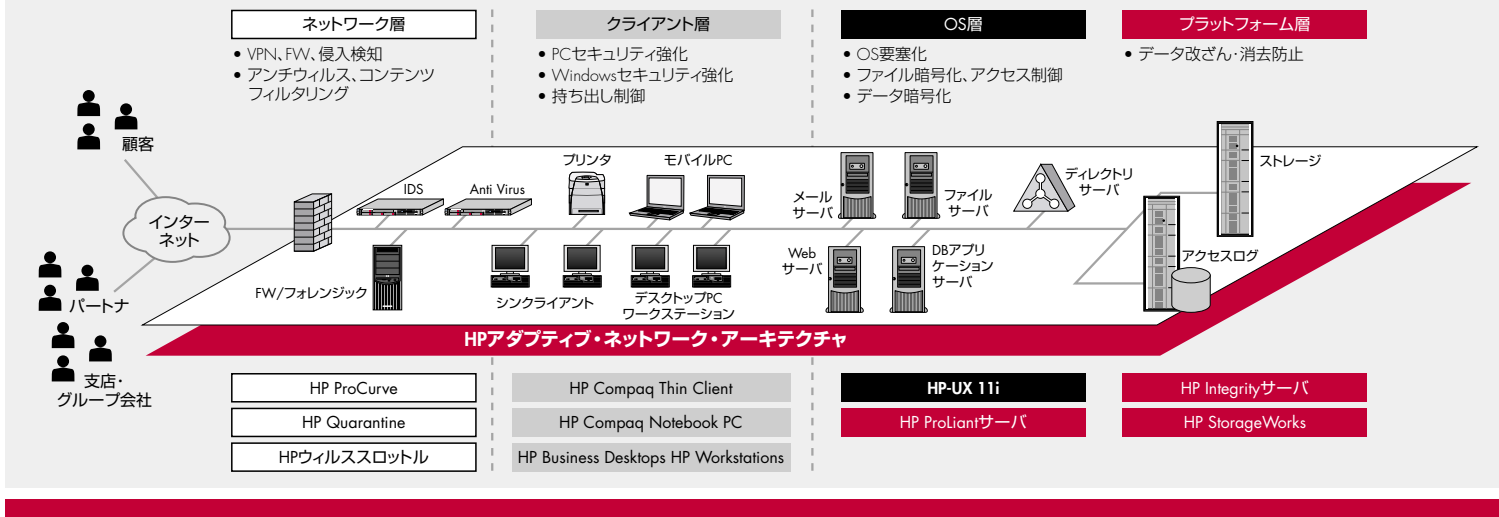
HP Integrityサーバは、世界中の企業でミッションクリティカルな環境に数多く採用され、日本でも社会インフラを支える重要なシステムで多くの実績を誇っています。特にセルボード・アーキテクチャを採用したHP SuperdomeおよびミッドレンジサーバはミッションクリティカルなHP Superdomeおよびミッドレンジサーバは、ミッションクリティカル環境に必要な可用性と信頼性、セキュリティ性を提供します。セルボード単位で構成可能な物理パーティションnPartitionは、それぞれを電気的に完全に分離でき、パーティション内の障害を完全に封じ込めることが可能です。パーティションは1台のサーバとして機能するため、開発環境と本番環境を1つのサーバ筐体内に効率的に実装し、アクセス制御や可用性確保の課題をハードウェアレベルで改善することも可能です。

また、エントリークラスおよびブレードサーバにオプションで提供される業界標準のセキュリティハードウェア TPM(Trusted Platform Module)は、HP-UXのファイル暗号化機能(EVFS)と組み合わせることで、ディスクの盗難による情報漏えいリスクに対応可能。ソフトウェアレベルのセキュリティ機能をハードウェアレベルでも補完し、セキュリティをさらに強化しています。

■ HP ProLiantサーバ

世界トップシェアを誇るx86サーバ、それがHP ProLiantサーバです。標準的なx86サーバにおいて、システムの信頼性の違いはハードウェア設計により顕著に現れます。HP ProLiantの内部は、独自に研究を重ねて設計したマザーボードを搭載。コンポーネント配置の最適化や、メンテナンス性も重視したケーブルレス設計、安定稼動のための冷却効率の最大化など、耐障害性に優れたハードウェアとしてシステムの可用性向上に貢献できるようにデザインされています。また、ハードウェア設計でも管理性を追及し、プロセッサやメモリのアップグレード、メンテナンスなどが容易に行えます。たとえば、コンポーネントに障害が発生した場合、障害箇所や各プロセッサ、メモリの状態、温度異常をLEDで指示します。さらに、ハードウェアに関するボトルネックの検出・分析を容易にする運用管理ソフトウェア「HP ProLiant Essentials」を提供するなど、業界標準アーキテクチャながらも、システムの信頼性を最大化させるための独自の工夫を随所に凝らしています。

■ HP StorageWorks

企業データの多くは、散在する契約書や文書ファイル、電子メール、アクセスログといった、管理が困難な「非構造化データ」とよばれるものです。HPのRISS(Reference Information StorageSystem)は、このような十分な管理が難しい情報に対する高いデータ保全性を実現するため、改ざんや不正消去防止の仕組み、グリッドテクノロジによる拡張性と可用性、電子署名の付与などのさまざまなセキュリティ機能をビルトイン。米国の厳しいデータ保管の法規制にも対応できるHPStorageWorksの信頼性は、すでに多くのお客様が実感しています。また、改ざん防止のWORM(Write Onece Read Many)機能をあらゆるライフサイクルステージのデータに提供できるよう、テープ製品やハイエンドディスクアレイにも搭載しています。

クライアント層

■ HP Compaq Thin Client

HP Compaq Thin Clientは、HP ブレードPCやブレードワークステーション、HP StorageWorksと組み合わせることで、データセンタに設置されたクライアントPC環境へのリモートアクセスを提供します。PCそのものをブレード化して集約し、画面情報のみを端末のシンクライアントに送信することで、ユーザ側に機密性の高い情報が散在し流動性を高めてしまうリスクを排除します。また、ソフトウェアライセンスに対する不正利用を防止して、一貫したバージョン管理と運用手順の確立を可能にします。また、各種サーバ・ベースド・コンピューティング環境のシンクライアント端末としてもご使用いただけます。

■ HP Compaq Notebooks・HP Business Desktops・HP Workstations

HPのビジネスPCは、重要データに対する不正アクセスや盗難をクライアントデバイスレベルで強力に保護します。HP Compaq Notebooksは、電界強度測定方式の最新型半導体リーダーを採用。指の表面より深い層にある真皮の部分を読み取ることができるため、正確な本人認証（本人認証率99.9%以上）が可能です。また、ハードディスクそのものに直接パスワードをかけるドライブロックにより、盗難の場合もディスクの読み込みには認証が必要となり、ハードディスク盗難による情報漏洩を防止できます。HP Business Desktops・HP Workstationsでは、BIOSで物理的にロックをかけることで、ハードディスクやメモリなどの盗難防止が可能です。この機能は導入時に一斉に設定可能で、各ユーザの設定に依存するリスクがありません。さらに、ログオン後のアクセスデータが、認可されていない第三者にアクセスされないよう、データ暗号化の際に生成される暗号鍵をOSやハードディスクと独立させて、セキュリティチップに格納・管理します。HPなら、昨今のビジネスPC環境に必須となったセキュリティ機能である「BIOS設定」「ドライブロック」「指紋認証」「スマートカード」「セキュリティチップ」などを提供するだけでなく、HPのビジネスPC共通のセキュリティ設定ソフトウェアである「HP Protect Tools」による一元的な管理が可能です。

ネットワークデバイス層

■ HP ウィルススロットル

従来型のワームやウィルス対策製品では、サードパーティから提供されるウィルスシグネチャで接続要求をモニタリングすることが多く、新種のウィルスには防御が不十分でした。HPの主力スイッチ製品であるProCurveソリューションでは、トラフィックがネットワークスイッチを通過する際にウィルス的に異常な動作を検出し、感染した機器のアクセススピードを低速化。さらに、感染したスイッチポートの完全な自動シャットダウンを実行します。同時に、ネットワーク管理者にはレポートが届き、原因と対応に必要なアクションを判断できます。HP ウィルススロットルは、ウィルスに感染したプロセスだけに関与するため、他のトラフィックに遅延などの障害を及ぼしません。HP ウィルススロットルは、ファイアウォールやアンチウィルスソフトウェアがウィルスを検出しない場合の追加レイヤとしての機能を提供するもので、HPのスイッチ製品「HP ProCurve」、「HP ProLiant」サーバ、「HP BladeSystem」アーキテクチャに提供されます。

ネットワークアーキテクチャ層

■ HPアダプティブ・ネットワーク・アーキテクチャ

ネットワークの広域帯化により、リソースの利用効率や運用管理効率を高める手段の1つとして、ネットワークの統合化が進んでいます。しかし、統合化による効率向上の一方で、一部に発生したセキュリティ上の問題が、統合されたネットワーク全体に波及するという新たなリスクを生み出すことがあります。HP アダプティブ・ネットワーク・アーキテクチャは、ネットワークの物理的区分けから、ビジネス要件に基づいた、アプリケーションやサービスごとの論理区画にネットワークを分割し、中央での一括したポリシー管理の下でコンパートメント単位のネットワーク統合・分割やアクセス制御を瞬時に変更できるアーキテクチャです。このモデルにより、事業分割、分社化や企業合併、新たな事業モデルに応じた外部接続などのビジネス変化に対して、セキュリティを妥協することなく、ビジネスを推進できるようになります。

〈HPが提供する主なソリューション〉

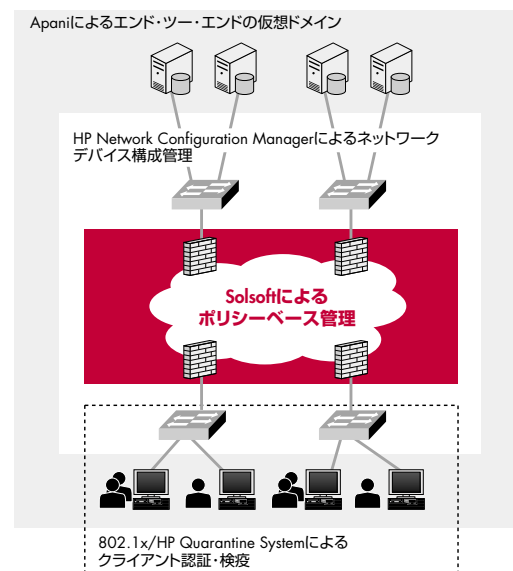
セキュアネットワーク・ソリューション

社内外の多様なネットワーク·アクセスを安全かつ柔軟に提供するには、多様なセキュリティ対策の実施に加えてシンプルな運用プロセスが必要になっています。HPのセキュアネットワーク·ソリューションは、ネットワークのセグメンテーション化やアプリケーショントラフィックのエンド·ツー·エンドの暗号化、認証認可機能と監査証跡機能などをネットワークにビルトイン。運用コストを抑制しながら安全かつ俊敏性の高いネットワーク·インフラを実現します。

●対象となるお客様

- 誰でも自由に繋げるフラットなネットワーク環境から、適切なガバナンスの利いたネットワークに移行したい
- DHCP、無線LANなどモビリティを有効活用し、ワーカの生産性を向上させたい

●ソリューションの特長

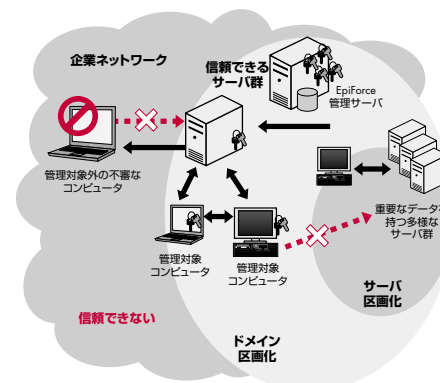
- 仮想閉域網、アクセス制御、クライアント認証といった対象の異なるセキュリティ対策を、統合的に、一貫性をもって提供

ネットワーク仮想閉域網ソリューション

ネットワークを論理的に分割し、より細かいグループ単位でITリソースへのアクセスを提供し、トラフィックをエンド·ツー·エンドで暗号化が可能です。また、監査証跡の一つとなるネットワークアクセスログの統合収集も可能です。

●対象となるお客様

- 本番環境と開発環境のアクセスを厳密に制限したい
- パートナや外部委託先のアクセスを限定したい
- レガシーシステムや特定のデータベースのトラフィックを暗号化したい
- 上記をグローバルに標準化して実装したい

●ソリューションの特長

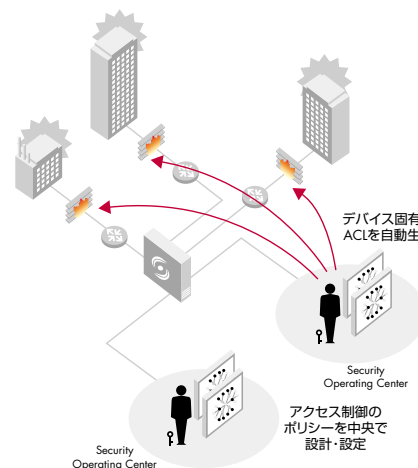
- 多様なプラットフォーム上のIP Secの幅広いサポート
- IP Secのアクセス·ポリシーを一元的に管理可能
- エンタープライズレベルの高拡張性
- HPによるグローバルデリバリ&サポート

ネットワーク·アクセス制御ポリシー·統合管理ソリューション

多様なネットワーク·セキュリティ機器のアクセス制御ポリシーを設計·実装·文書化するには、膨大で複雑な人的対応が必要です。これを統合化·自動化することで、一貫性のあるアクセス制御ポリシーを網羅的に反映することができます。マルチベンダ機器で余儀なくされていたデバイスベースの管理をポリシーベースに移行でき、運用負荷を増やすことなく、複雑なネットワーク環境を管理することができ、攻撃へのレスポンス向上も図れます。

●対象となるお客様

- デバイスルールを整理して、セキュリティホールを解消したい
- 重大ウィルス発生時に緊急強制ルールを瞬時に全体展開したい
- 多様なネットワーク機器に一貫性のあるポリシを反映したい
- ネットワーク機器に共通のセキュリティ管理指針に移行し、コンプライアンスの効率化を図りたい

●ソリューションの特長

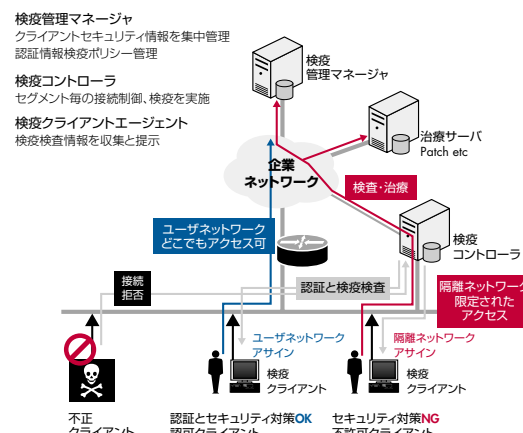
- マルチベンダ&マルチデバイスに共通の管理インタフェースで、統合ポリシー管理を実現
- セキュリティ·インシデント&イベント管理ツールとの連携により、インシデント対応の高速化·効率化が可能
- 変更管理の履歴記録とロールバックに対応

クライアント認証・検疫ソリューション

クライアント認証・検疫ソリューションは、HP Quarantine Systemによりクライアントの認証・認可を行い、阻止すべきクライアントアクセスを自動検知し一時的に隔離します。さらに、HP Softwareをはじめとするソフトウェア配布ツールと連携のうえ、必要なパッチを強制適用して接続を可能にします。ユーザの生産性を阻害することなく、ウィルス等が原因の情報漏えいやサービス妨害を未然に防止することができます。

●対象となるお客様

- マルチOSの大規模クライアント環境で、認証・アクセス制御をしたい
- 社内ネットワークに接続する全てのクライアントが、ポリシー準拠できているか把握・対策したい

●ソリューションの特長

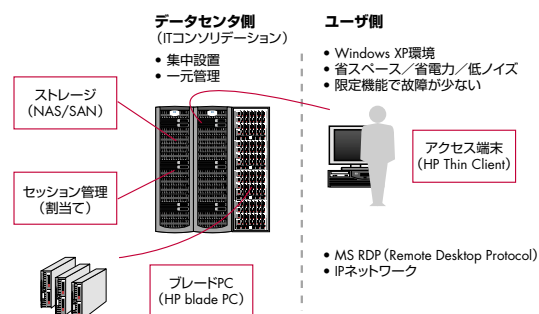
- MACアドレスベースの管理により、種類や世代の制限なくネットワーク接続を行う全てのクライアントの認証が可能
- クライアントの構成やOSパッチ、ウィルスソフトの適用状況に関する検査を実施
- 既存のネットワーク環境に短期間で導入可能

HP クライアントPC統合（CCI）ソリューション

HP クライアントPC統合ソリューションは、演算部、記憶部をデータセンタに集約することで、物理的な社外へのデータ持ち出しを防ぎます。クライアントPCからはデータへのアクセスのみを許可し、ファイルの保存やプリントアウト操作を許可しない厳格なクライアントセキュリティ環境を運用することができます。

●対象となるお客様

- デスクトップPCに対して高いセキュリティ対策と統合的な管理をしたい企業・組織
- 広範囲にPCやキオスク端末を展開しながら、IT管理者の工数が不足しがちな企業・組織
- 顧客データなど守秘性の高いデータを個人が扱う部門
- 大規模に専門的な用途を行なうデスクトップPCを設置している企業
- 派遣社員比率が多いなど、人材流動性が高い組織
- 授業のカリキュラムが頻繁に変わる教育機関

●ソリューションの特長

- クライアントと併せてストレージも集約されるため、高いセキュリティレベルとシステム継続性を実現
- Microsoft Remote Desktop Protocol（RDP）などの標準技術を採用し、データセンタへのBlade PCの集約性を高められる
- PCからワークステーションまで幅広いユーザ要求に対応

HPセキュリティ・ソリューションの特長

企業ユーザとしての豊富な経験に基づく製品開発

HPのセキュリティソリューションは、企業ユーザとしてのHPが経験したITセキュリティのベストプラクティスを、幅広い製品ラインナップとコンサルティング・システム構築・運用サービスに反映し、グローバルのお客様を支援しています。

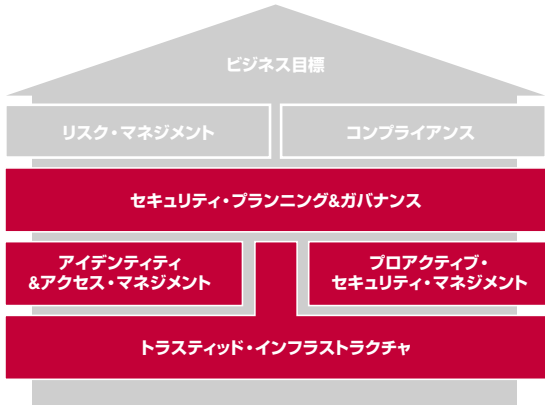
多様なセキュリティ技術の標準化推進

HPでは、セキュリティ技術の多層化の重要性と同時に複雑化するセキュリティメカニズムの改善の必要に気付き、これを業界全体の問題として提唱してきました。そしてITをリードするベンダの1つとして、Liberty Alliance, TCG, OASISなどの業界標準団体に参画しており、数多くのセキュリティ関連ISVとともに、積極的な情報交換、新技術の開発や標準化推進に貢献しています。

セキュリティ・エンジニア育成への取り組み

HPでは、全世界でCISSP（Certified Information Systems Security Professionals）の育成に積極的な投資を行なっています。国内では、業界第2位の有資格者数を誇り、最適なITセキュリティ環境構築に努めています。

IT基盤構築に向けた包括的な製品・サービス提供

エンタープライズのITインフラストラクチャの運用・システム構築・テクノロジを総合的に提供するHPでは、IT機器から次世代データセンタ基盤の構築に及ぶ様々な製品・サービスのご提供を展開しています。HPのセキュリティ・ソリューションとあわせて、エンタープライズのIT基盤構築にむけた包括的なご支援が可能です。

安全に関するご注意　ご使用の際は、商品に添付の取扱説明書をよくお読みの上、正しくお使いください。水、湿気、油煙等の多い場所に設置しないでください。火災、故障、感電などの原因となることがあります。

お問い合わせはカスタマー・インフォメーションセンターへ
03-6416-6660 月〜金 9:00〜19:00　土 10:00〜18:00（日、祝祭日、年末年始および5/1を除く）
HP セキュリティ・ソリューションに関する情報は http://www.hp.com/jp/security

本カタログは環境保護のため100%再生紙および大豆インキを使用しています。

invent

日本ヒューレット・パッカード株式会社
〒102-0076 東京都千代田区五番町7番地

JSL07128-01